学校编码: 10384　　　　分类号: ________ 密级: ________
学　　号: 19020070153846　　　　UDC: _______

厦门大学

博 士 学 位 论 文

Galois 理论与 McKay 猜想

Galois Theory and the McKay Conjecture

陈晓友

指导教师姓名: 曾吉文 教授
专 业 名 称: 基 础 数 学
论文提交日期: 2010 年 4 月
论文答辩时间: 2010 年 6 月
学位授予日期: 2010 年 月

答辩委员会主席: ____________________
评　　阅　　人: ____________________

2010 年 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　　　　　　　　　　　　　）课题（组）的研究成果，获得（　　　　　　　　）课题（组）经费或实验室的资助，在（　　　　　　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）:

年　月　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于:

（　　　）1. 经厦门大学保密委员会审查核定的保密学位论文，于　　年　月　日解密，解密后适用上述授权。

（　　　）2. 不保密，适用上述授权。

（请在以上相应括号内打”√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　月　日

摘　　要

Galois 理论是代数学的一个重要和活跃的分支. 我们在第一章中介绍了一些关于 Galois 理论的基本内容, 并且提出了二次正则类的定义, 得到了一些关于它的性质. Galois 理论的这些基本内容在后面的章节中会多处用到.

Brauer 特征标在模表示理论中扮演着重要角色. 我们在第二章中建立和说明了超-Brauer 特征标的概念, 并证明了如下结论.

设 $\mathscr{K}$ 与 $\mathscr{Y}$ 分别为 G^0 和 $\mathrm{IBr}(G)$ 的划分, 且假定 Brauer 特征标 δ_Y 在 $K \in \mathscr{K}$ 上取常值, 其中 $Y \in \mathscr{Y}$, 则 $|\mathscr{Y}| \leq |\mathscr{K}|$. 如果 $|\mathscr{Y}| = |\mathscr{K}|$, 则有

(a) Brauer 特征标集合 $\{\delta_Y \mid Y \in \mathscr{Y}\}$ 生成一个在 $\mathscr{K}$ 的成员上取常值的定义在 G^0 上的复值函数空间.

(b) 划分 $\mathscr{Y}$ 决定 $\mathscr{K}$, 并且 $\mathscr{K}$ 是唯一最粗糙的与 $\mathscr{Y}$ 相谐调的 G^0 的划分. 特别地, $\mathscr{K}$ 的成员是正则共轭类的并.

(c) $\mathscr{K}$ 的某个成员恰由 G 的单位元组成, 而 $\mathscr{Y}$ 的某个成员恰由 G 的主 Brauer 特征标组成.

(d) 如果 r 是一个与 $|G|_{p'}$ 互素的正整数并且 $g \in G^0$, 则映射 $g \mapsto g^r$ 诱导出 $\mathscr{K}$ 上的一个置换.

(e) 若 G 为 p-可解群并且划分 $\mathscr{K}$ 也唯一确定 $\mathscr{Y}$, 则复数域 $\mathbb{C}$ 的每一个自同构诱导出 $\mathscr{Y}$ 上的一个置换.

由 R. Brauer 创立和发展的块论在有限群理论中起着重要的作用. 我们在第三章中讨论了块的一些基本性质以及块包含, 并且得到了如下结论.

设 D 为有限群 G 的 p-子群且假设 $U \lhd G$ 包含在 D 中. 设 $b \in \mathrm{Bl}(\mathbf{N}_G(D)|D)$ 且记 $\bar{G} = G/U$, 其中 $\mathrm{Bl}(\mathbf{N}_G(D)|D)$ 表示 $\mathbf{N}_G(D)$ 的以 D 为亏群的块的集合, 则 b^G 包含唯一的从 $\mathbf{N}_G(D)/U$ 诱导 的 $\bar{G}$ 的块当且仅当 b 包含唯一的 $\mathbf{N}_G(D)/U$ 的块.

在第四章中, 我们介绍了 McKay 猜想的发展概况, 并且针对一个特定的零散单群 M_{11} 我们进行了 Navarro 块猜想的验证.

关键词: Galois 理论　二次正则类　超-Brauer 特征标　块　McKay 猜想

Abstract

Galois theory is an important and active branch of algebra. We introduce some basic facts about Galois theory, present the definition of quadratic regular class, and obtain some properties on it in Chapter one. We utilize these rudiments of Galois theory in the next chapters and sections.

Brauer characters play a crucial role in modular representation theory. We establish and illustrate the concept of super-Brauer character and we prove the following in Chapter two.

Let $\mathscr{K}$ and $\mathscr{Y}$ be partitions of G^0 and of $\mathrm{IBr}(G)$*, respectively, and assume that the Brauer characters δ_Y for $Y \in \mathscr{Y}$ are constant on $K \in \mathscr{K}$. Then $|\mathscr{Y}| \leq |\mathscr{K}|$. If $|\mathscr{Y}| = |\mathscr{K}|$, then the following hold.*

(a) *The Brauer characters δ_Y for $Y \in \mathscr{Y}$ span the space of all complex-valued functions on G^0 that are constant on the members of $\mathscr{K}$.*

(b) *The partition $\mathscr{Y}$ determines $\mathscr{K}$, and $\mathscr{K}$ is the unique coarsest partition of G^0 which is compatible with $\mathscr{Y}$. In particular, the members of $\mathscr{K}$ are unions of regular conjugacy classes.*

(c) *Some member of $\mathscr{K}$ consists of just the identity of G and some member of $\mathscr{Y}$ consists of just the principal Brauer character of G.*

(d) *If r is a positive integer which is coprime to $|G|_{p'}$ and $g \in G^0$, then the map $g \mapsto g^r$ induces a permutation on $\mathscr{K}$.*

(e) *If G is a p-solvable group and the partition $\mathscr{K}$ also determines $\mathscr{Y}$, then every automorphism of the complex field $\mathbb{C}$ induces a permutation on $\mathscr{Y}$.*

Block theory which is established and developed by R. Brauer plays an important part in finite group theory. We discuss some essential properties about blocks and inclusion of blocks, also we obtain the following in Chapter three.

Let D be a p-subgroup of a finite group G and suppose that $U \lhd G$ is contained in D. Let $b \in \mathrm{Bl}(\mathbf{N}_G(D)|D)$ and write $\bar{G} = G/U$, where $\mathrm{Bl}(\mathbf{N}_G(D)|D)$ denotes the set of blocks of $\mathbf{N}_G(D)$ with defect group D. Then b^G contains a unique block of $\bar{G}$ which is induced from $\mathbf{N}_G(D)/U$ if and only if b contains a unique block of $\mathbf{N}_G(D)/U$.

In Chapter four, we introduce developments of the McKay conjecture, and we verify the Navarro block conjecture for a specific sporadic simple group M_{11}.

Key Words: Galois theory; quadratic regular class; super-Brauer character; block; McKay conjecture

目　　录

Contents

绪　论

E. Galois 在十九世纪三十年代初为了解决代数方程是否可用根号解的问题而引进了置换群的概念, 这标志着群论的产生. 所谓用根式解方程的问题就是一个多项式的根如何用它的系数经过有限次的四则运算和开方表示出来, 这是十九世纪以前代数的一个主要问题. 人们在古巴比伦时代就已经知道一元二次方程的解法. 但是三次与四次方程直到公元一千五百年左右才由 Ferro, Tartaglia, Cardano 和 Ferrari 等人先后给出解的公式. 从此, 人们致力于五次以上方程的根式解法, 但经过三百年的努力一直未能成功. 这期间 Lagrange, Ruffini 和 Abel 都作出了卓越的贡献. 一八二四年, 数学家 Abel 证明了一般五次方程不能用根式解, 但是他并没有解决什么时候一个方程可用根式解, 什么时候不能用根式解这样的问题. E. Galois 在悉心研究了 Lagrange, Abel 和 Gauss 的著作之后, 将方程的群定义为全部根的置换所组成的集合, 由此他将多项式的根可用根式解的条件转化为多项式的群应该是可解的. 这样, E. Galois 用他自己创立的群论彻底地解决了这个问题. E. Galois 的工作不仅漂亮地解决了一元 n 次方程的根式解问题, 而且开创了代数学的新纪元. 关于 E. Galois 杰出工作的详细介绍, 可参看 B. L. van der Waerden 的名著 [121].

和群论有紧密联系的 Galois 理论就是 E. Galois 创立的解方程的理论. 运用 Galois 理论, 不仅可以解决一元 n 次方程是否可用根式求解问题, 而且还为解决古典数学三大难题提供了非常漂亮和简洁的方法. 关于 Galois 理论的第一个全面而清晰的介绍是 C. Jordan 给出的. 代数学家 E. Artin 写了一部很经典的关于 Galois 理论的著作 [5]. 按照 E. Galois 原创想法的方式, 即, 仿照 E. Galois 的思想, H. M. Edwards 写出了著作 [48]. P. Morandi [93] 主要从域论的一些内容开始逐步地介绍 Galois 理论及其应用. Galois 理论是代数学中一个活跃的分支, 即使是有限 Galois 理论也有许多至今仍未解决的难题. 比如给定一个有限群, 是否存在一个有理数域 $\mathbb{Q}$ 上的多项式使得其 Galois 群同构于给定的群? 已知对可解群, 对称群和交错群有肯定的回答, 但对一般情况还没有令人满意的答案. 上面的问题就是所谓的 Galois 逆问题, 由此所形成的理论称为逆 Galois 理论. 为此, G. Malle 与 B. H. Matzat 专门写了著作 [88].

一八七零年以前, 只有置换群和几何变换群被研究. 关于交换群的公理化定义是由 L. Kronecker 在一八七零年给出的, 而有限群的公理化定义是由 H. Weber 在一八八二年给出的. 第一部关于有限群的专著 [28] 是由 W. Burnside 于一八九七年写出的. H. Zassenhaus 也有一部很著名的关于群论的著作 [128]. 群论现已有许多分支, 如有限群论, 李群论, 代数群论, 无限群论等等; 其中有限群论是近世代数中历史最长, 内容最丰富的分支之一. 自从 E. Galois 引入群之后, 代数学的研究方向逐渐转向研究各种代数结构. 有限交换群基本定理称任一有限交换群总是一些循环子群的直积. 由这个基本定理, 有限交换群的分类就清楚了. 对于任一有限群 G, 可做出次正规群列

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_{n-1} \rhd G_n = 1.$$

如果 G_i/G_{i+1} 为单群, 其中 $i \in \{0, 1, \ldots, n-1\}$, 此时这个群列称为合成列, 而 G_i/G_{i+1} 称为 G 的合成因子. Jordan-Hölder 定理称若群 G 有两个合成列, 则在不计次序的情况下, 合成因子一一同构. 这样一来, 有限单群就可以看作一般有限群的基石. 根据 Jordan-Hölder 定理有限群的分类与结构可以归结为: 单群的分类与结构, 以及群的扩张问题. 可否把全部有限单群找出来? 通过众多代数学家的努力, 总算于一九八一年完成了有限单群的分类. H. Kurzweil 与 B. Stellmacher 在他们的著作 [82] 中给出了有限单群分类定理.

任一有限单群必同构于下列群中之一:

1. 素数阶循环群;
2. 交错群 $A_n, n \geq 5$;
3. 典型线性群:
$\mathrm{PSL}_n(q)$, $\mathrm{PSU}_n(q)$, $\mathrm{PSp}_{2n}(q)$, 或 $\mathrm{PO}_n^{\varepsilon}(q)$;
4. 例外 Lie 型群:
${}^3D_4(q)$, $E_6(q)$, ${}^2E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, ${}^2F_4(2^n)$, $G_2(q)$, ${}^2G_2(3^n)$, 或 ${}^2B_2(2^n)$
5. 零散单群:
M_{11}, M_{12}, M_{22}, M_{23}, M_{24} (Mathieu 群);
J_1, J_2, J_3, J_4 (Janko 群);
Co_1, Co_2, Co_3 (Conway 群);
HS, Mc, Suz;
Fi_{22}, Fi_{23}, Fi'_{24} (Fischer 群);
F_1, F_2, F_3, F_5; He, Ru, Ly, ON.

另外, M. Aschbacher 与 D. Gorenstein 分别在其著作 [10] 与 [60] 中也列举了已知的有限单群. 关于有限单群的著作, 可参看 M. Aschbacher [11] 与新近出版的 R. A. Wilson 的作品 [123].

有限单群理论是同有限群理论大致平行发展的, 所用的工具也大致相同, 它的发展中有几个重要的突破点. 一九五五年, R. Brauer 与 K. A. Fowler 在 [21] 中发现对合的中心化子的关键作用. 他们发现若群 G 中的对合的中心化子已知, 那么单群 G 只有有限多种可能性. 从而若再适当选定 G 的对合的中心化子, 则就有可能得到新的单群, 这就是系统刻画偶阶群的方法, 它被称为 Brauer 纲领. 一九六三年, W. Feit 与 J. G. Thompson 在 [52] 中证明了 W. Burnside 的猜想, 即, 奇数阶群是可解的. 这个定理的证明使得 Brauer 纲领得以实施. 一九七零年以后, 群论专家 D. Gorenstein 开始酝酿有限单群完全分类纲领, 他于一九七二年提出了一个十六步的可操作方案. 到一九八一年二月, D. Gorenstein 正式宣布有限单群的分类完成.

人们在寻找有限单群的过程中发展了表示理论这个强有力的工具. J. J. Rotman 在其著作 [111] 的后记中写道如果想更深入地研究群论, 必须学习表示论. 因为利用表示可以将抽象群中的元素以及运算具体化, 这样就有助于我们了解抽象群的各种性质, 特别是它的结构. 表示即是指群 G 到 $\mathrm{GL}_n(F)$ 的同态, 其中 F 是代数封闭域. 当 F 的特征不整除 $|G|$ 时, 因为任意 FG 模都是完全可约模, 这种情况下讨论群 G 的表示理论, 就称为常表示理论. 特别地, 当 $F = \mathbb{C}$ 时, 如果 $\mathfrak{X} : G \to \mathrm{GL}_n(\mathbb{C})$ 是一个同态, 则对每个 $g \in G$ 就有 $\mathfrak{X}(g)$ 是一个 $n \times n$ 复矩阵. 这个表示的特征标定义为

$$\chi : G \to \mathbb{C}, \quad g \mapsto \mathrm{tr}(\mathfrak{X}(g)).$$

此时特征标和表示在相似意义下相互唯一确定. 有限群特征标理论是由 F. G. Frobenius 于一八九六年在研究群行列式时创立的, 在一八九七年他发表了关于有限群表示理论的第一篇文章. 同年, W. Burnside 写出了关于有限群理论的第一部著作. T. Y. Lam 在一九九八年专门写了两篇文章 [83, 84] 来纪念表示论的创立. 并且, C. W. Curtis 专门写了一部著作 [33] 来介绍表示论的先驱们以及他们的工作.

有限群复表示的基本理论几乎由 F. G. Frobenius 和 W. Burnside 完成. I. Schur 后来利用现在所称的 Schur 引理简化了 Frobenius 的复杂的理论. 特征标理论提供了一种利用环论技术来研究有限群的方法. 特征标理论为证明关于有限群的定理提供了强大的工具. 特征标理论为 Burnside 的 p^aq^b 阶群为可解群的定理提供了一个简洁有力的证明, 而几十

年后其纯群论的证明先由 D. M. Goldschmidt 在 [59] 中给出了部分证明, 随后, H. Bender 才在 [12] 中给出了关于 p^aq^b 阶群为可解的完整的纯群论证明. 如果有限群 G 的非平凡真子群 H 满足对任意的 $x \in G - H$ 有 $H \cap H^x = 1$, 则 H 称为 G 的 Frobenius 补, 而 G 称为 Frobenius 群. 设 H 为 G 的 Frobenius 补, 利用特征标理论可以证明

$$\{1\} \cup (G - \cup_{x\in G} H^x) = N$$

为 G 的正规子群且 $NH = G$, $N \cap H = 1$. 这就是 Frobenius 定理. 虽然利用特征标理论早已将这个定理证明, 但是至今没有纯群论的证明.

D. E. Littlewood 于一九五零年在其著作 [87] 中介绍了有限群特征标理论和矩阵表示. C. W. Curtis 的著作 [32] 为有限群表示理论提供了一个很完整的介绍. J.-P. Serre 使用很简洁的语言在著作 [113] 中介绍了常表示理论. 关于特征标理论方面的其他参考文献可见 [2, 45, 50, 67, 78]. 而 I. M. Isaacs 的著作 Character Theory of Finite Groups, 即 [70], 是我们本文写作的主要参考文献之一. I. M. Isaacs 在其著作中阐述了一系列的特征标理论及其应用, 他曾把特征标理论分为六个研究专题, 当然也是他最感兴趣的一些专题, 即

特征标对应;
Brauer 特征标;
π-特殊特征标;
M-群;
特征标次数;
线性群.

B. Huppert 在 [68] 中介绍了表示论中的一些相关研究内容, 其中有很多涉及到了特征标次数. 关于特征标对应, G. Navarro 于一九九四年在 [100] 中介绍了一系列的公开问题以及相关的进展. 另外, Ya. G. Berkovich 与 E. M. Zhmud′ 的著作 [13, 14] 对特征标理论中一些问题也给出了总结. Brauer 特征标在专著 [58] 与 [99] 中都有被介绍和讨论.

如果前面提到的域 F 的特征整除群 G 的阶时, 所得到的理论称为模表示理论. L. E. Dickson 首先称特征为素数 p 的域上的表示为模表示, 他指出如果域 F 的特征不整除 $|G|$, 则常表示和模表示没有本质区别. L. E. Dickson 在其文章 [42, 43, 44] 中给出了一些评论和例子说明了, 若域 F 的特征整除 $|G|$ 时, 情况就大不相同. 在二十世纪初期, I. Schur 就已开始研究群的模表示理论. 另一方面, 由 E. Noether 以及其他一些数学家发展的代数理论使得有限群表示理论的研究可以从环和模的观点进行. 系统地研究模表示及其对群结构的应用, 是由 R. Brauer 于二十世纪三十年代开始的. 现在模表示理论已经成为代数学的一个重要分支. 二十世纪六十年代, J. A. Green 在其文章 [62] 中利用模论方法发展了模表示. 随后, J. G. Thompson 利用 J. A. Green 的理论给出了两个应用. J. A. Green 的方法也被 E. C. Dade 用来发展了循环亏群理论. J. L. Alperin 的著作 [1] 以及 P. Landrock 的专著 [85] 都是用模论观点来写表示论的. 另外, L. Dornhoff 的教材 [46] 以及 R. Gow 与 B. Huppert 等人的著作 [61] 也较详细地介绍了模表示理论. 比较中立和全面的介绍模表示的教材是 H. Nagao 与 Y. Tsushima 的专著 [95], 而 W. Feit 的作品 [51] 则是关于模表示理论的最全面的专著.

模表示的一个特点是未必完全可约, 即不可分解表示不一定是不可约表示, 因此, 在考虑表示的结构时, 除了考虑不可约表示之外, 还要考虑不可分解表示. (不可分解表示是指不能分解成两个真子表示的直和的表示.) R. Brauer 在 [22] 中给出了 G 的不可约模表示的个数等于 p-正则类的个数的定理. 所以对于有限群 G 来说, 不可约的模表示是有限个, 但不可分解的模表示却有无限多个, 情况要复杂的多. 而对于 G 的正则表示的直和分解中所出现的不可分解表示的个数却是有限的, 并且恰好等于不可约表示的个数. 设 F 是

特征为素数 p 的代数闭域, G 为有限群, $p\big||G|$, 再设 $\mathfrak{Y}: G \to \mathrm{GL}_n(F)$ 为表示, 则

$$\varphi^*: G \to F, \quad g \mapsto \mathrm{tr}(\mathfrak{Y}(g))$$

为对应于 $\mathfrak{Y}$ 的迹函数. 这个迹函数有时不能反映表示的性质, 特别是表示的次数. 而 R. Brauer 思想的深刻之处在于他引进了现在称为 Brauer 特征标的类函数, 使得模表示的一些信息可以在复数域里获得. 这个概念是在文献 [22] 中引入的, 同样在这篇文献中, R. Brauer 和 C. Nesbitt 建立了块论里的一些基本事实. 紧接着, R. Brauer 与 C. Nesbitt 又在文献 [23, 16] 中研究了 Brauer 特征标的性质以及它和常特征标的联系. 正如 R. Brauer 在文献 [20] 中所写的那样, 我们希望在群的块和群的结构之间找到一些关系. 事实上, R. Brauer 正是利用块论得出了很多关于单群结构的成果. 关于 R. Brauer 的生平及工作的详细介绍, 可参看文献 [34, 35] 及 C. W. Curtis 的专著 [33].

在 R. Brauer 一九六三年发表的文章 [19] 中, 他列举了有限群表示论里面的一系列问题. 到目前为止, 其中的大部分问题都没有获得解决. 顺便地, 我们介绍几个.

Brauer 11 问题: *给定群 G 的特征标表, 能从中获得 G 的子群的多少信息?*

Brauer 19 问题: *用群 G 的群论性质刻画 G 的亏零块的个数.*

Brauer 20 问题: *是否有 $|\mathrm{Irr}(B)| \le p^{\mathrm{d}(B)}$?*

Brauer 23 问题: *是否有 $\mathrm{Irr}(B) = \mathrm{Irr}_0(B)$ 当且仅当 B 的亏群交换?*

其中 Brauer 20 问题就是 Brauer $\mathrm{k}(B)$-猜想, 而 Brauer 23 问题就是 Brauer 高零猜想. J. L. Alperin 在文献 [3] 中指出块论的主要问题是:

如果 G 是有限群, 利用 p-局部子群给出一些简单的法则来决定出特征标在 p-奇异元上的值.

而且在那篇文献中, J. L. Alperin 提出了 McKay 猜想的一般形式以及关于块的一个猜想. B. Külshammer 在文献 [81] 中用例子阐述了有限群表示论里的一些重要猜想以及它们之间的联系, 并且他的专著 [80] 也是块论方面的一本重要参考文献. 关于有限群表示论发展的一些趋势, 可参看 J. L. Alperin 与 M. Broué等人写的文章 [4].

国内的模表示理论始于数学家段学复, 他曾用群的模表示理论来探讨单群的结构并取得了卓越的成果, 见文献 [24, 119]. 数学家段学复为我国群表示理论方面培养了许多研究专家, 其中有很多专家取得了很好的成绩.

对一个有限群 G 来说, 其亏零块在对群 G 的研究中起着很重要的作用. 关于亏零块的存在性以及刻画, 可参看 S. M. Shi [114]. 利用块的一些性质来刻画群的性质是 R. Brauer 所感兴趣的一个专题. 最近, C. Bessenrodt 与 J. P. Zhang 在 [15] 中使用块分离给出了幂零群的一个等价刻画. Brauer 高零猜想是群表示论中的一个热点问题, 这个猜想已知对于 p-可解群是成立的, 而且对于具有正规亏群的块也是成立的. Y. Fan 与 B. Külshammer 在 [49] 中给出了具有交换亏群的块的一些结论. 对于一个块, 它有许多不变量, 利用这些不变量可以对群的性质给出一些刻画. 而估计这些不变量之间的关系也是人们经常考虑的问题. 关于块中的一些不变量, J. W. Zeng 在 [129] 中证明了一个与这些不变量有关的不等式.

下面我们来介绍一下本文的具体的框架以及主要内容.

我们在第一章第一节中介绍 Galois 理论, 重点是 Galois 理论的基本定理 1.12. 虽然这个定理在介绍 Galois 理论的书中都会涉及, 我们还是倾向于把这个证明写出来. 另外一个定理 1.13, 在后面的应用中显得非常重要, 因此我们也把它的证明写出来了. 这其中涉及到的群论内容, 可参看 I. M. Isaacs 的新作 [72] 或者百科全书式的 B. Huppert 的三

卷 [64, 65, 66]. 在第二节中, 我们讨论分圆域, 其中我们把分圆多项式在有理数域 $\mathbb{Q}$ 上是不可约的证明写了出来, 因为这个结论对于后面的应用起着重要的作用. 设 G 为有限群, $\mathrm{Irr}(G)$ 表示 G 的不可约 (复) 特征标的集合, $\mathrm{cl}(G)$ 表示 G 的共轭类的集合. 设 $K \in \mathrm{cl}(G)$, $g \in K$, $\mathbb{Q}(K) = \mathbb{Q}(\psi(g) \mid \psi \in \mathrm{Irr}(G))$, 称 K 为二次的 (quadratic), 如果 $|\mathbb{Q}(K) : \mathbb{Q}| = 2$. 设 $\chi \in \mathrm{Irr}(G)$, $\mathbb{Q}(\chi) = \mathbb{Q}(\chi(g) \mid g \in G)$, 称 χ 为二次的, 如果 $|\mathbb{Q}(\chi) : \mathbb{Q}| = 2$. G. Navarro 在 [103] 中证明了奇数阶群的二次共轭类与二次不可约特征标的个数相同. 我们在第三节中给出的一个群的特征标表显示这对于偶阶群是不成立的. 我们原来想将第四节放到第二章去, 但是感觉这部分内容和 Galois 理论联系较为紧密, 因此我们把这一节留在了第一章中. 在这一节中用到的 Brauer 特征标的一些具体性质可参看第二章第一节.

设 G 为有限群, p 为一固定的素数, G^0 表示 G 的 p-正则元集合, $\mathrm{cl}(G^0)$ 表示 p-正则元所在的共轭类的集合, 即正则共轭类集合. 类似于 G. Navarro 的定义, 称 $L \in \mathrm{cl}(G^0)$ 为二次的 **(quadratic)**, 如果

$$|\mathbb{Q}(L) : \mathbb{Q}| = |\mathbb{Q}(\varphi(x) \mid x \in L, \varphi \in \mathrm{IBr}(G)) : \mathbb{Q}| = 2,$$

其中 $\mathrm{IBr}(G)$ 表示 G 的不可约 p-Brauer 特征标集合. 我们证明了如下结论:

定理 1.49 *设 G 为奇阶有限群, p 是整除 $|G|$ 的固定素数. 假设 $L \in \mathrm{cl}(G^0)$ 且 $y \in L$. 若 L 是二次的, 则 y 是 q-元, 其中 $q \neq p$ 为素数.*

设 $\varphi \in \mathrm{IBr}(G)$, 称 φ 为**二次的**, 如果

$$|\mathbb{Q}(\varphi) : \mathbb{Q}| = |\mathbb{Q}(\varphi(x) \mid x \in G^0) : \mathbb{Q}| = 2.$$

如果 $p\big||G|$, 我们找到了使得二次正则类与二次不可约 Brauer 特征标的个数不相同的例子. 但对于奇数阶群, 我们却无法说明二次正则类与二次不可约 Brauer 特征标的个数是否相同.

第二章第一节主要介绍了 Brauer 特征标的定义及其性质. 在有限群表示理论中, 表示的扩张问题是人们较多关注的对象. 设 F 为代数封闭域, $N \lhd G$, $\mathfrak{X} : G \to \mathrm{GL}_n(F)$ 为群 G 的不可约 F-表示, 人们通常会去关注 $\mathfrak{X}$ 限制到 N 上还是否不可约? 利用常特征标来说的话就是, 如果 $\psi \in \mathrm{Irr}(N)$, 且存在 $\chi \in \mathrm{Irr}(G)$ 使得 $\chi_N = \psi$, 则称 ψ 可扩张. 如果 ψ 是 N 的 G-不变不可约特征标, 且 N 为 G 的正规 Hall-子群, 则 ψ 必可扩张. 对于不可约 Brauer 特征标, 也有相同的性质, 即, 如果 $\varphi \in \mathrm{IBr}(N)$ 为 G-不变不可约 Brauer 特征标, 且 N 为 G 的正规 Hall-子群, 则存在 $\alpha \in \mathrm{IBr}(G)$ 使得 $\alpha_N = \varphi$.

若 $\varphi \in \mathrm{IBr}(G)$, F 是特征为素数 p 的代数封闭域, 则 φ 在相似意义下唯一确定不可约表示 $\mathcal{X} : G \to \mathrm{GL}_n(F)$, 从而 φ 唯一确定 F-表示

$$\det(\mathcal{X}) : G \to F^{\times}, \quad g \mapsto \det(\mathcal{X}(g)).$$

这个表示唯一地确定 G 的一个线性 Brauer 特征标, 记为 $\det(\varphi)$. 可否利用这个定义来给出一个不可约 Brauer 特征标可扩张的等价条件呢? 基于此, 我们得到了下面的结论.

定理 2.20 *设 $N \lhd G$, G/N 可解. 又设 $\theta \in \mathrm{IBr}(N)$ 是 G-不变的, $(|G : N|_{p'}, \theta(1)) = 1$, 则 θ 可扩张到 G 当且仅当 $\det(\theta)$ 可扩张到 G.*

P. Diaconis 与 I. M. Isaacs 于 2008 年在 [40] 中阐述了超特征标理论. 假定群 G 与其不可约特征标集合 $\mathrm{Irr}(G)$ 被分别划分为非空子集的族 $\mathcal{K}$ 与 $\mathcal{X}$. 假设对于每个 $X \in \mathcal{X}$, 存在一个特征标 χ_X, 其不可约成分均在 X 中, 并且使得下面的假定成立:

(a) $|\mathcal{K}|=|\mathcal{X}|$;
(b) 特征标 χ_X 在 $\mathcal{K}$ 的成员上取值为常值;
(c) $\{1\}\in\mathcal{K}$.

则 χ_X 称为**超特征标 (supercharacter)**, 而 $\mathcal{K}$ 中成员称为**超类 (superclass)**. 并且, 对于群 G 来说, 划分 $\mathcal{X}$ 与 $\mathcal{K}$, 加之选取的那些特征标 χ_X 形成一个**超特征标理论 (supercharacter theory)**, 只要上面的 (a), (b) 与 (c) 成立.

我们在文献 [29] 中考虑了 Brauer 特征标, 并且提出了超-Brauer 特征标理论. 设 G 为有限群, p 为一固定素数, G^0 为 G 的 p-正则元集合, $\mathrm{IBr}(G)$ 为 G 的不可约 p-Brauer 特征标集合. 方便起见, 我们分别称 p-正则元和 p-Brauer 特征标为正则元和 Brauer 特征标. 假设 $\mathrm{IBr}(G)$ 和 G^0 分别被划分为非空子集的族 $\mathscr{Y}$ 和 $\mathscr{K}$, 且假定对每个 $Y\in\mathscr{Y}$, 存在一个 Brauer 特征标 θ_Y 使得其不可约 Brauer 成分均在 Y 中, 并且使得下列条件成立:

(a) $|\mathscr{Y}|=|\mathscr{K}|$;
(b) θ_Y 在 $\mathscr{K}$ 的成员上取常值;
(c) $\{1\}\in\mathscr{K}$.

则称 θ_Y 为**超-Brauer 特征标**, 而 $\mathscr{K}$ 的成员为**超-正则类**. 并且称 $\mathscr{Y}$ 和 $\mathscr{K}$ 以及上面选定的 Brauer 特征标 θ_Y 形成一个关于 G 的**超-Brauer 特征标理论**, 如果它们满足上面的三个条件. 我们在第二节中给出了一系列的可能存在超-Brauer 特征标理论的例子, 其中一些涉及具体的群, 另外一些涉及到 Brauer 置换引理以及 Galois 自同构.

我们在第三节中给出了下列结论的证明.

定理 2.26 *设 $\mathscr{K}$ 与 $\mathscr{Y}$ 分别为 G^0 和 $\mathrm{IBr}(G)$ 的划分, 且假定 Brauer 特征标 δ_Y 在 $K\in\mathscr{K}$ 上取常值, 其中 $Y\in\mathscr{Y}$, 则 $|\mathscr{Y}|\le|\mathscr{K}|$. 如果 $|\mathscr{Y}|=|\mathscr{K}|$, 则有*

(a) Brauer 特征标集合 $\{\delta_Y \mid Y\in\mathscr{Y}\}$ 生成一个在 $\mathscr{K}$ 的成员上取常值的定义在 G^0 上的复值函数空间.

(b) 划分 $\mathscr{Y}$ 决定 $\mathscr{K}$, 并且 $\mathscr{K}$ 是唯一最粗糙的与 $\mathscr{Y}$ 相谐调的 G^0 的划分. 特别地, $\mathscr{K}$ 的成员是正则共轭类的并.

(c) $\mathscr{K}$ 的某个成员恰由 G 的单位元组成, 而 $\mathscr{Y}$ 的某个成员恰由 G 的主 Brauer 特征标组成.

(d) 如果 r 是一个与 $|G|_{p'}$ 互素的正整数并且 $g\in G^0$, 则映射 $g\mapsto g^r$ 诱导出 $\mathscr{K}$ 上的一个置换.

(e) 若 G 为 p-可解群并且划分 $\mathscr{K}$ 也唯一确定 $\mathscr{Y}$, 则复数域 $\mathbb{C}$ 的每一个自同构诱导出 $\mathscr{Y}$ 上的一个置换.

我们在第三章第一节中介绍了块论里的一些基本事实. 自从引入块之后, R. Brauer 研究的中心主题就变为块论及其到有限群的应用, 特别是到有限单群分类问题的应用了. R. Brauer 的思想是利用块论去获得满足一定条件的不可约特征标的值. Brauer 第二主定理的一个很漂亮的应用就是: 设 $|G|=pqr^m$, 其中 p,q,r 为三个不同的素因子. 如果 G 为单群, 则 $|G|=60$ 或者 $|G|=168$. 另外, 对于常特征标来说, 第一和第二正交关系是很重要的. 设 G 为有限群, $\mathrm{Irr}(G)$ 表示 G 的不可约特征标的集合, 则

$$[\chi,\psi]=\frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\psi(g)}=\delta_{\chi\psi},$$

其中 $\chi, \psi \in \mathrm{Irr}(G)$, $\delta_{\chi\psi}$ 为 Kronecker 函数. 这就是第一正交关系. 第二正交关系如下:

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\overline{\chi(h)} = |\mathbf{C}_G(g)|,$$

如果 g 与 h 在 G 中共轭; 否则为 0. 通俗地讲, 块就是一个等价类, 其中包含有不可约特征标和不可约 Brauer 特征标. 对于块来说, 同样有两个正交关系. 设 x 为 G 的一个 p-元, 称 $S_p(x) = \{g \in G \mid g_p$与 x 在 G 中共轭$\}$ 为 G 的一个 p-截面 (p-section). 设 $\chi, \psi \in \mathrm{Irr}(G)$ 位于两个不同的块中, 则对任意的 p-截面有

$$\sum_{g \in S_p(x)} \chi(g)\overline{\psi(g)} = 0.$$

下面这个就是著名的块正交关系.

$$\sum_{\chi \in \mathrm{Irr}(B)} \chi(g)\overline{\chi(h)} = 0,$$

其中 B 为 G 的一个块, g_p 与 h_p 在 G 中不共轭.

我们知道商群的特征标可以看作大群上的特征标, 因此商群的块就与大群的块存在一定的关系. 我们在第二节中介绍了块包含的一些相关信息. G. Navarro 在 [101] 中证明了如下结论.

设 D 为群 G 的 p-子群, 假设 $U \lhd G$ 包含在 D 中, 令 $\bar{G} = G/U$. 设 $b \in \mathrm{Bl}(\mathbf{N}_G(D)|D)$, 其中 $\mathrm{Bl}(\mathbf{N}_G(D)|D)$ 表示 $\mathbf{N}_G(D)$ 的以 D 为亏群的块的集合, 且假定 $\bar{b} \in \mathrm{Bl}(\mathbf{N}_G(D)/U)$. 如果 $\bar{b}$ 包含在 b 中, 则 $\bar{G}$ 的块 $\bar{b}^{\bar{G}}$ 包含在 G 的块 b^G 中.

事实上, 上面的结论可用图表

$$\begin{tikzcd} \bar{b}^{\bar{G}} \arrow[r, "\subseteq"'] & b^G \\ \bar{b} \arrow[u] \arrow[r, "\subseteq"] & b \arrow[u] \end{tikzcd}$$

来表示. 我们在这一节中证明了如果先有上图中上面的包含, 那么也可得到上图中下面的包含. 实际上, 我们给出了如下结论.

定理 3.25 *设 D 为有限群 G 的 p-子群且假设 $U \lhd G$ 包含在 D 中. 设 $b \in \mathrm{Bl}(\mathbf{N}_G(D)|D)$ 且记 $\bar{G} = G/U$, 则 b^G 包含唯一的从 $\mathbf{N}_G(D)/U$ 诱导的 $\bar{G}$ 的块当且仅当 b 包含唯一的 $\mathbf{N}_G(D)/U$ 的块.*

对于表示或者特征标来说, 人们首先感受到的数量是其次数, 因此关于特征标次数方面的研究内容比较丰富. 我们在第四章中的讨论就是涉及特征标次数的内容.

设 G 为有限群, p 为一固定的素数, $P \in \mathrm{Syl}_p(G)$, **McKay 猜想**断言

$$|\,\mathrm{Irr}_{p'}(G)| = |\{\chi \in \mathrm{Irr}(G) \mid p \nmid \chi(1)\}| = |\{\psi \in \mathrm{Irr}_{p'}(\mathbf{N}_G(P)) \mid p \nmid \psi(1)\}| = |\,\mathrm{Irr}_{p'}(\mathbf{N}_G(P))|.$$

其中 $\mathbf{N}_G(P)$ 表示 P 在 G 中的正规化子. 这个猜想已被验证对于许多种类的群都是成立的, 然而其一般性的证明却没有人揭示出来. 事实上, 因为 P/P' 为 $\mathbf{N}_G(P)/P'$ 的正规交换 Sylow p-子群, 由 Ito 定理可知对任意 $\psi \in \mathrm{Irr}(\mathbf{N}_G(P)/P')$ 有 $p \nmid \psi(1)$. 所以

$$\mathrm{Irr}(\mathbf{N}_G(P)/P') \subseteq \mathrm{Irr}_{p'}(\mathbf{N}_G(P)).$$

现在, 设 $\phi \in \mathrm{Irr}_{p'}(\mathbf{N}_G(P))$, 从而 ϕ_P 的不可约成分均为线性的, 于是 $P' \subseteq \ker\phi \cap P \subseteq \ker\phi$, 因此

$$\mathrm{Irr}_{p'}(\mathbf{N}_G(P)) \subseteq \mathrm{Irr}(\mathbf{N}_G(P)/P').$$

即 McKay 猜想断言

$$|\,\mathrm{Irr}_{p'}(G)| = |\,\mathrm{Irr}_{p'}(\mathbf{N}_G(P))| = |\,\mathrm{Irr}(\mathbf{N}_G(P)/P')|.$$

J. L. Alperin 把 Mckay 猜想放到了块上来考虑了. 设 $B \in \mathrm{Bl}(G|D)$, $\mathrm{Irr}(B) = \mathrm{Irr}(G) \cap B$. **Alperin-McKay 猜想**声称

$$|\,\mathrm{Irr}_0(B)| = |\{\chi \in \mathrm{Irr}(B) \mid \mathrm{height}(\chi) = 0\}| = |\{\psi \in \mathrm{Irr}(b) \mid \mathrm{height}(\psi) = 0\}| = |\,\mathrm{Irr}_0(b)|,$$

其中 $b \in \mathrm{Bl}(N_G(D)|D)$ 是 B 的 Brauer 对应量, 即 $b^G = B$. 如果 Alperin-Mckay 猜想获得证明, 那么 McKay 猜想就自动成立了.

G. Navarro 在 [101] 中提出了一个关于块的猜想, 现在称之为 Navarro 块猜想. 设 G 为 n 阶有限群, p 为一素数, e 为一非负整数, $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ 将每个 p'-单位根 ξ 映到 ξ^{p^e}. 假设 $B \in \mathrm{Bl}(G|D)$, $b \in \mathrm{Bl}(\mathbf{N}_G(D))$ 使得 $b^G = B$, **Navarro 块猜想**宣称

$$|\,\mathrm{Irr}_0^\sigma(B)| = |\{\chi \in \mathrm{Irr}_0(B) \mid \chi^\sigma = \chi\}| = |\{\psi \in \mathrm{Irr}_0(b) \mid \psi^\sigma = \psi\}| = |\,\mathrm{Irr}_0^\sigma(b)|.$$

当 $\sigma = 1$, Navarro 块猜想即是 Alperin-McKay 猜想. G. Navarro 在 [101] 中证明了 Navarro 块猜想对于具有循环亏群的块是成立的. 我们在第二节中针对一个特定的零散单群 M_{11} 给出了 Navarro 块猜想的验证.

我们注意到 Navarro 块猜想中所用到的 Galois 自同构是我们在第一章中提到的群 $\mathcal{H}$ 中的元, 从而这些自同构可以作用到不可约 Brauer 特征标上去. 若 G 为 p-可解群, 根据 T. R. Wolf 的定理, 始终有

$$|\,\mathrm{IBr}_0(B)| = |\{\varphi \in \mathrm{IBr}(B) \mid \mathrm{height}(\varphi) = 0\}| = |\{\theta \in \mathrm{IBr}(b) \mid \mathrm{height}(\theta) = 0\}| = |\,\mathrm{IBr}_0(b)|,$$

其中 b 为 B 的 Brauer 对应量. 于是下面的问题就自然产生了.

问题 4.5 *设 G 为 n 阶 p-可解群, $B \in \mathrm{Bl}(G|D)$, $b \in \mathrm{Bl}(\mathbf{N}_G(D)|D)$ 满足 $b^G = B$. 又设 e 为一非负整数, $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ 将每个 p'-单位根 ξ 映到 ξ^{p^e}, 是否一定有*

$$|\,\mathrm{IBr}_0^\sigma(B)| = |\{\varphi \in \mathrm{IBr}_0(B) \mid \varphi^\sigma = \varphi\}| = |\{\theta \in \mathrm{IBr}_0(b) \mid \theta^\sigma = \theta\}| = |\,\mathrm{IBr}_0^\sigma(b)|?$$

第 一 章 Galois 理论

我们将在本章中介绍 Galois 理论的一些基本知识, 特别是 Galois 理论基本定理. 另外, 我们将重点地关注分圆域的一些内容. 在第三节与第四节中, 我们将讨论二次共轭类, 奇数阶群以及二次正则类. 关于 Galois 理论方面的内容的参考文献可见 E. Artin 与 A. N. Milgram [5], H. M. Edwards [48], D. S. Dummit 与 R. M. Foote [47], I. M. Isaacs [71], P. Morandi [93], J. J. Rotman [112] 以及 L. C. Washington[122].

§1.1 Galois 理论的基本定理

关于代数方程求解的理论就称为 Galois 理论. Galois 理论是代数学的一门重要分支. 有限 Galois 理论建立了域的有限扩域的相对自同构群与有限扩域之间的关系以及相互作用, 对解决扩域中的一系列问题起了关键作用. E. Galois 把这两个看似互不相干的领域沟通起来了, 很巧妙地在这两者之间建立了某种一一对应关系.

对于群来说, 我们常常会关注其子群的一些问题; 而对于域, 我们经常去关注那些包含固定域的更大的域, 这即是所谓的域扩张.

定义 1.1 如果 F 是域 E 的子域, 则称 E 是 F 的扩域, 记作 E/F. 若 X 为 E 的一个非空子集, 则 E 中包含 F 和 X 的一切子域的交称为在 F 上添加 X 得到的子域或称为 X 在 F 上生成的子域, 记作 $F(X)$.

命题 1.2 设 E/F 为域扩张, $F \subseteq L, M \subseteq E$ 为中间域, 以 LM 或 $\langle L, M\rangle$ 表示由 L, M 生成的子域, 则

(a) 若 $L = F(X)$, 其中 $X \subseteq E$, 则 $LM = M(X)$.

(b) $LM = L \cup M$ 当且仅当 $L \supseteq M$ 或 $M \supseteq L$.

证明 (a) 因 $X \subset L$, 故 $M(X) \subseteq LM$. 另一方面, $X \subseteq M(X)$, $F \subseteq M$, 所以 $L = F(X) \subseteq M(X)$, 从而 $LM \subseteq M(X)$.

(b) 只需证必要性. 若 L 与 M 互不包含, 则有 $a \in L\backslash M$, $b \in M\backslash L$, 那么 $ab \in LM = L \cup M$, 矛盾. ■

下面我们介绍一下分裂域, 正规扩域以及可分的概念.

定义 1.3 设 F 为域, F-多项式 $f(x)$ 的分裂域是指 F 的扩域 E, 在其中 $f(x)$ 可以完全分裂成一次因式之积且 $E = F(\{\alpha \in E \mid f(\alpha) = 0\})$.

定义 1.4 设 E/F 为域扩张, $\alpha \in E$. 如果存在 F-多项式 $f(x)$ 使得 $f(\alpha) = 0$, 则称 α 在 F 上是代数的. 若 E 中的每个元在 F 上都是代数的, 称 E/F 为代数扩张. 域 F 的代数扩域 E 称为在 F 上是正规的, 如果任意不可约 F-多项式只要在 E 中有根, 就在 E 中完全分裂为一次因式之积; 或等价地, 如果 E 中任意元所对应的极小多项式在 E 上分裂. (注意到, 二次扩张均为正规扩张.)

定义 1.5 设 F 为域, $f(x)$ 为不可约 F-多项式. 若 $f(x)$ 无重根则称 $f(x)$ 是可分的, 否则就称为不可分的. 若 $f(x)$ 的互异的根只有一个, 即 $f(x)$ 在其分裂域中分成形如 $a_0(x-u)^m$, 则称 $f(x)$ 为纯不可分的.

定义 1.6 设 E/F 为域扩张, $\alpha \in E$, 则 α 在 F 上是可分的, 如果 α 的极小多项式在 F 上是可分的. 若 E 中的每个元在 F 上都是可分的, 则称 E 在 F 上可分.